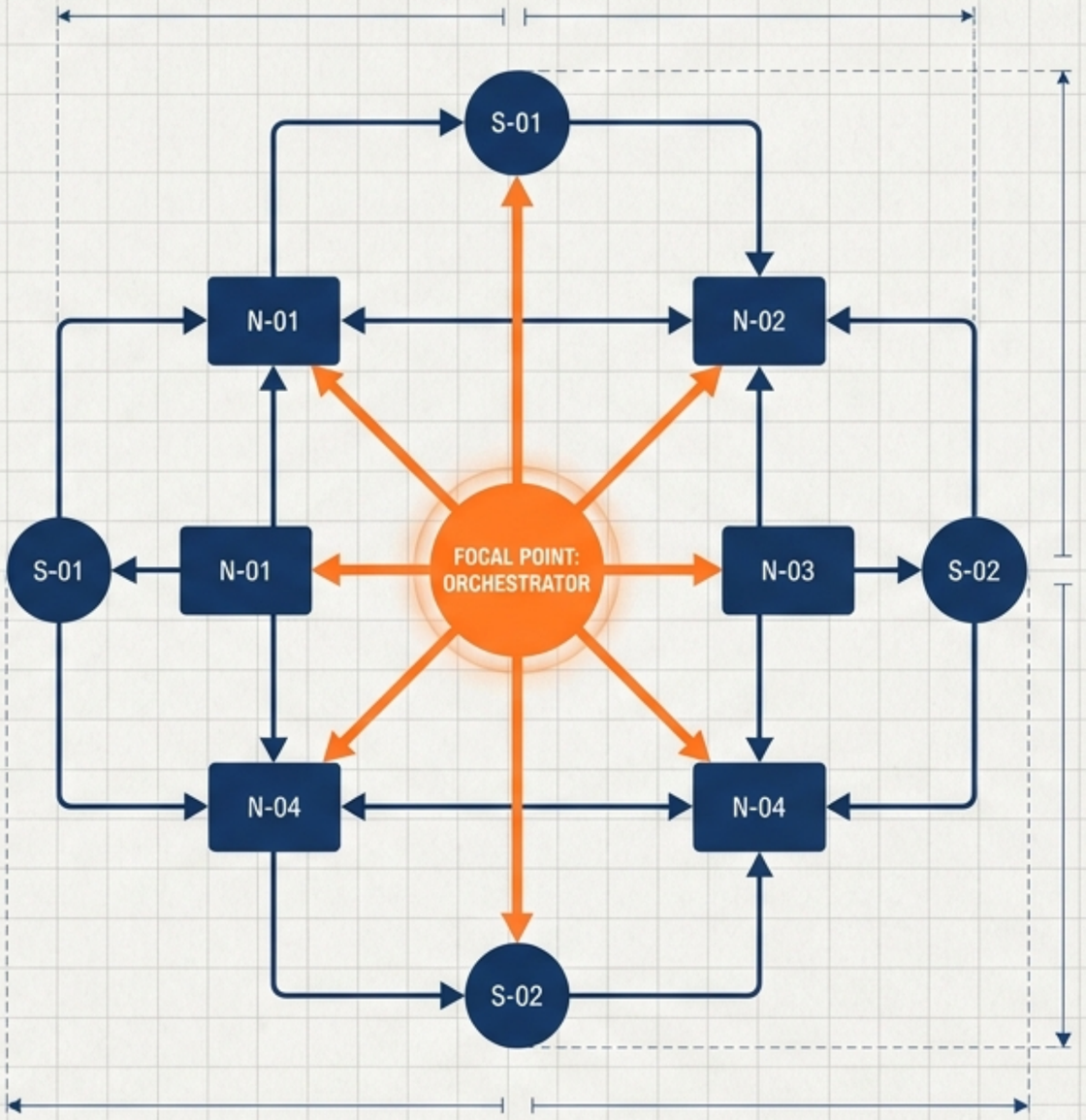
AI 智能体编排基础设施演进：基于 LangGraph 的多智能体系统　系统深度战略研究

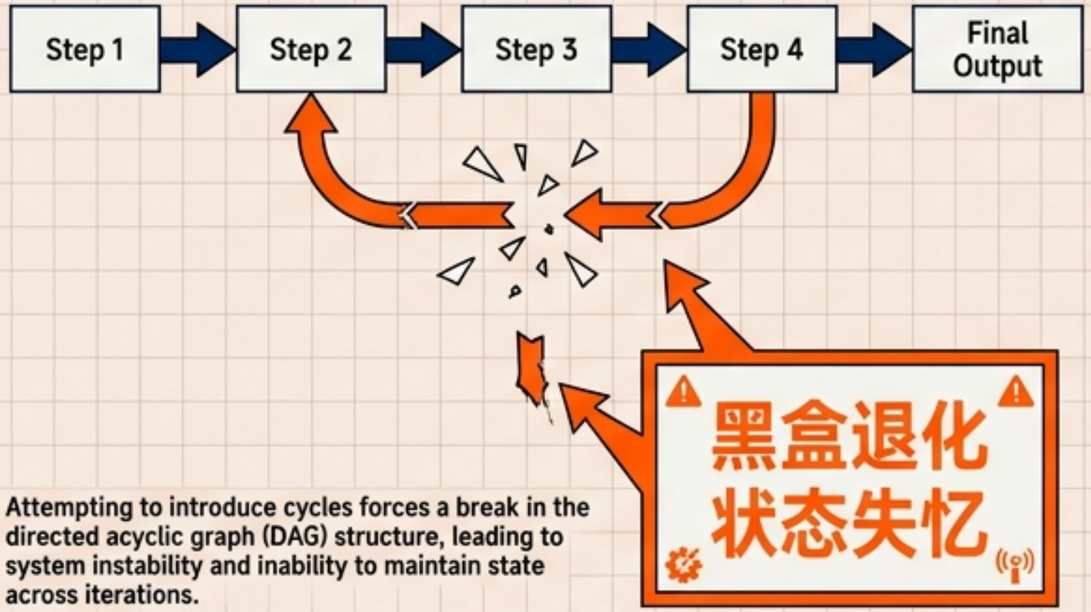
从线性流水线到确定性图计算——企业级复杂业务落地的架构重构



AI 产品总监面试呈现

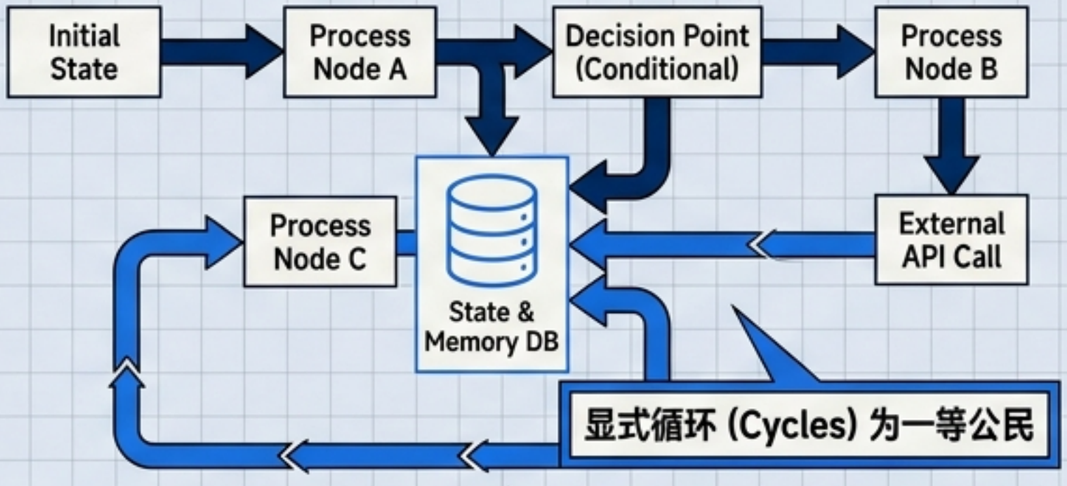
单一 Prompt → 线性流水线 (DAG) → 多智能体网络 (Multi-Agent)

LangChain 线性架构局限



Attempting to introduce cycles forces a break in the directed acyclic graph (DAG) structure, leading to system instability and inability to maintain state across iterations.

LangGraph 确定性降维打击



Cycles are explicitly modeled as first-class citizens, enabling state persistence, iterative processing, and self-correction without breaking the structural integrity.

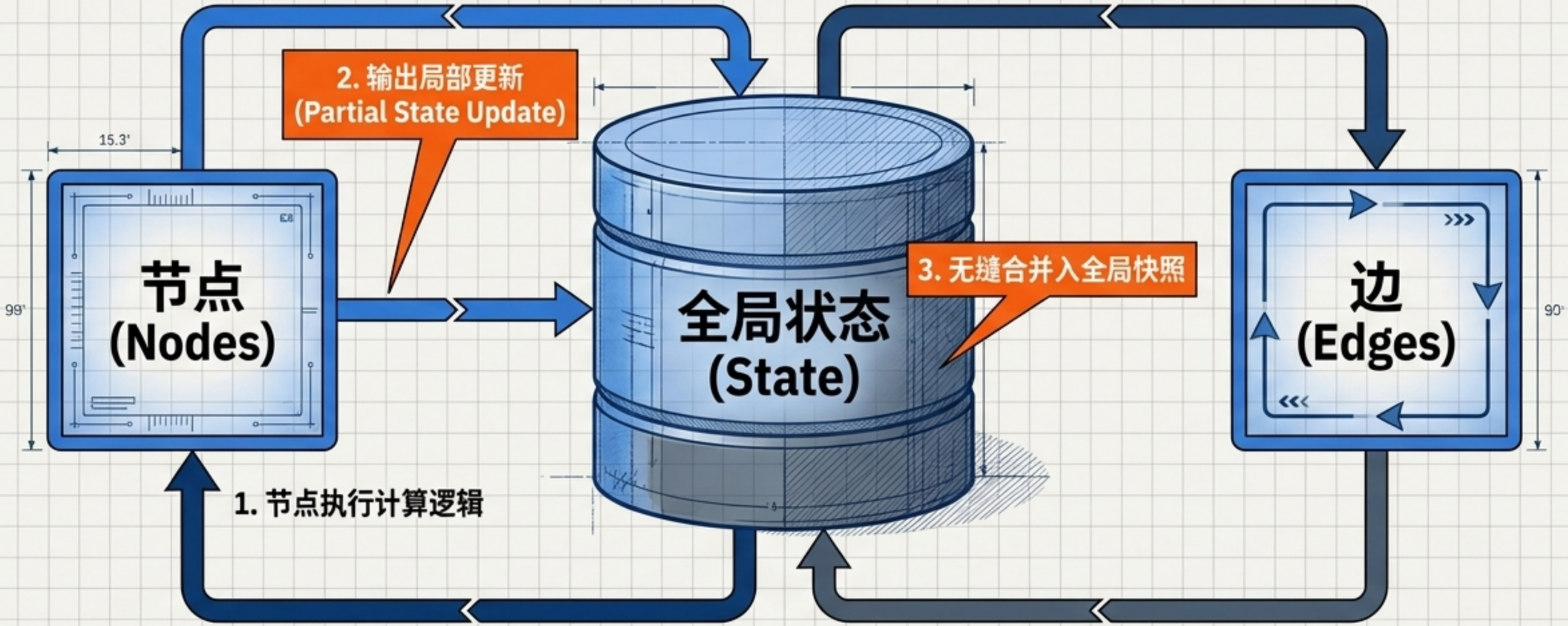
88% - 95%

复杂长线任务完成率稳定提升区间

ENGINEERING SPECIFICATION DOCUMENT

DRAWING NO:	REVISION:	DATE:
ARCH-2045	1.0	2024-05-15

系统记忆：全局状态 (System Memory: Global State) Hub-and-Spoke 架构



连贯记忆中央机制
统一真理来源

TITLE:
ENGINEERING SPECIFICATION DOCUMENT
DRAWING NO: ARCH-2045
REVISION: 1.0
DATE: 2024-05-15

函数节点 (Function)

标准 Python/JS 基础业务逻辑

可运行节点 (Runnable)

无缝兼容嵌入 LangChain 处理链

基于类的节点 (Class-Based)

维护复杂内部配置（__init__ 注入，__call__ 执行）

异步节点 (Async)

全面支持 I/O 密集型任务高并发处理

企业级运行时元数据 (RunnableConfig)

线程标识 (Thread ID)	超时限制 (Timeouts)	资源消耗成本 (Cost)
TID-0xA1B2C3D4	300.00 s / 5.00 min	$0.0042 / Op

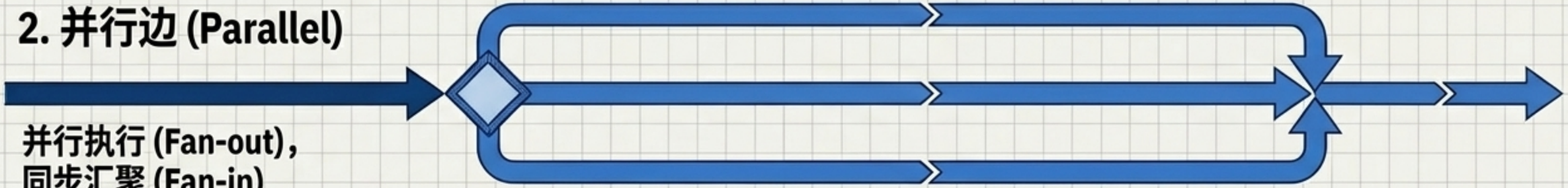
TITLE:
ENGINEERING SPECIFICATION DOCUMENT
DRAWING NO: ARCH-2047
REVISION: 1.0
DATE: 2024-05-15

系统流程控制：边缘与安全 (System Flow Control: Edges & Safety)

1. 无条件边 (Unconditional)

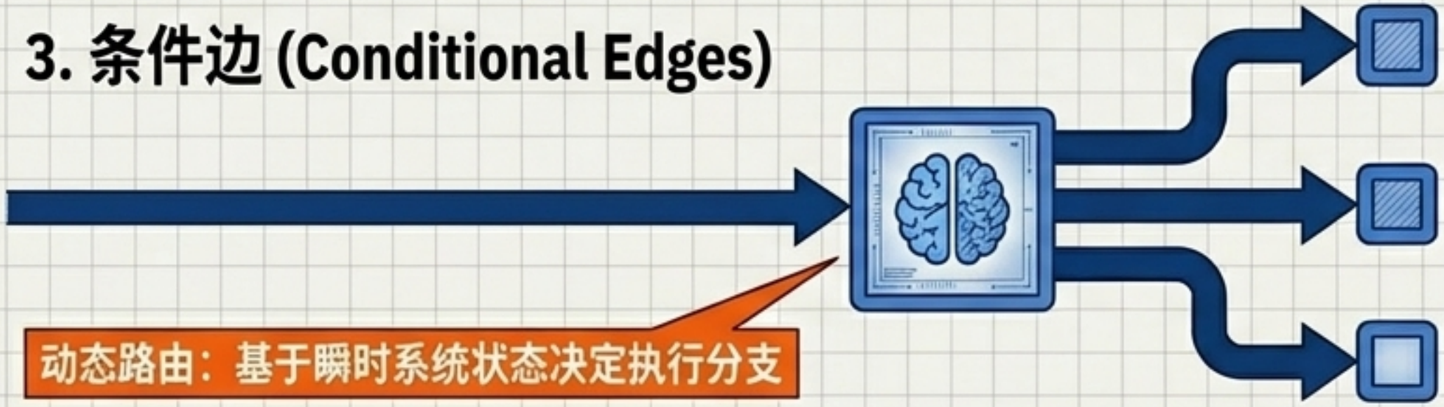
简单直接的线性流转

2. 并行边 (Parallel)



并行执行 (Fan-out)，
同步汇聚 (Fan-in)

3. 条件边 (Conditional Edges)



动态路由：基于瞬时系统状态决定执行分支

类型安全护栏 (Type-Safe Routing)

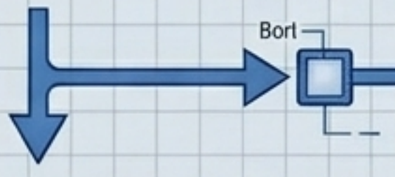
基于 Python Literal 强制静态类型检查
确保目标键值合法，实现 0 运行路由迷失

TITLE: ENGINEERING SPECIFICATION DOCUMENT		
DRAWING NO.: ARCH-2047	REVISION: 1.0	DATE: 2024-05-15

核心技术基石 (Core Technical Foundation)

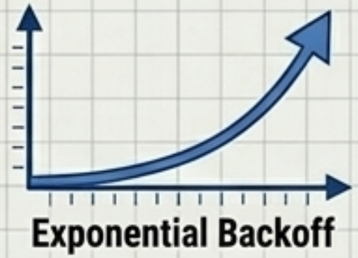
极致细粒度控制

- Command API：节点内聚路由跳转，减少外部条件边依赖

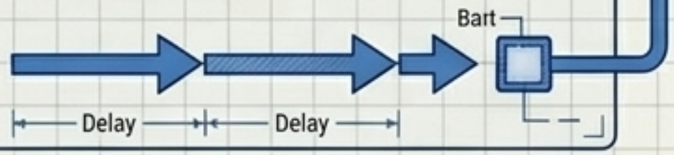


- Send API：专为动态分发的 Map-Reduce 架构设计

高可用容错网络

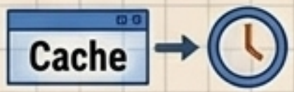


- Retry Policies：抗击大模型 API 限流与 500 错误
- 配置指数退避因子、最大尝试次数及抖动参数

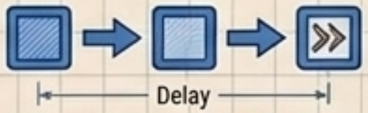


底层性能优化

- TTL 缓存阻击高频昂贵调用

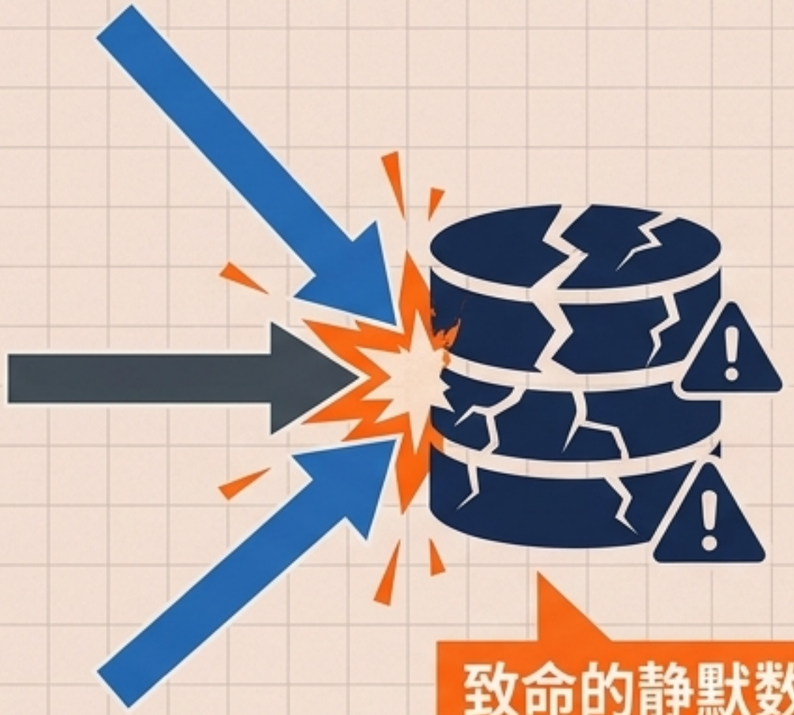


- defer=True 推迟非紧急任务（日志清理/通知）



THLE:		
ENGINEERING SPECIFICATION DOCUMENT		
DRAWING NO.: ARCH-2047	REVISION 1.0	DATE 2024-05-15

并发竞态灾难（最后写入者胜出）



致命的静默数据丢失

上下文泄漏风控：死循环追加会导致 Token 撑爆

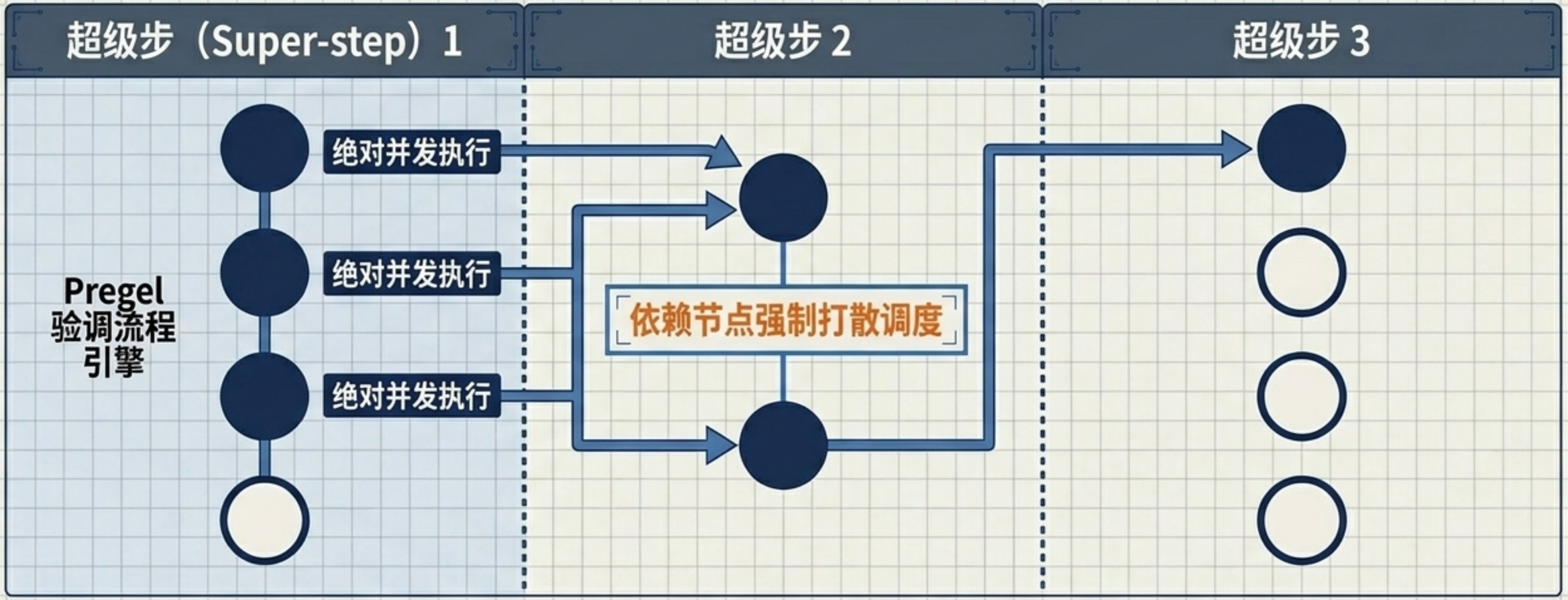
CRDT 归约器（Reducers）引擎

```
add_messages: Reducer[list[BaseMessage], BaseMessage] =
    lambda left, right: left + right
```

复杂合并护城河：smart_merge_dict（深层合并）& combine_distinct（严格去重）

ENGINEERING SPECIFICATION DOCUMENT	DRAWING NO. ARCH-2047	REVISION 1.0	DATE 2024-05-15

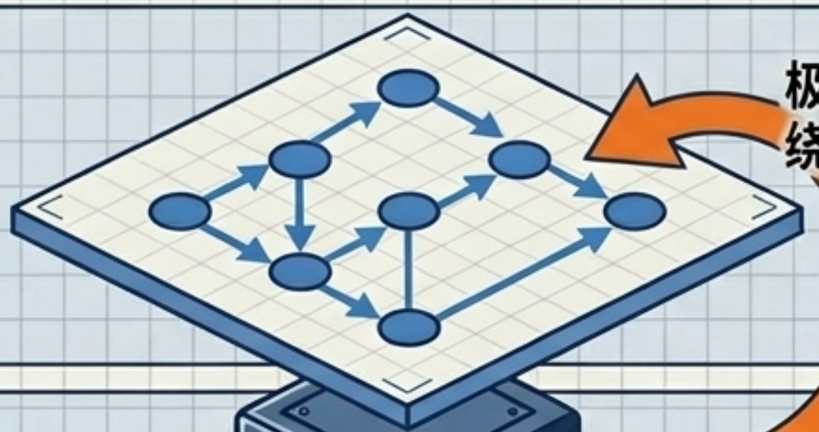
底座颠覆：Pregel 启发式离散消息传递算法



容错与状态管理：Checkpointer 深度快照机制

代码层（内存工作流）

极端环境容错：基于专属 Thread ID，
绕开推倒重来，断电/OOM后精准续传



Checkpointer 拦截器

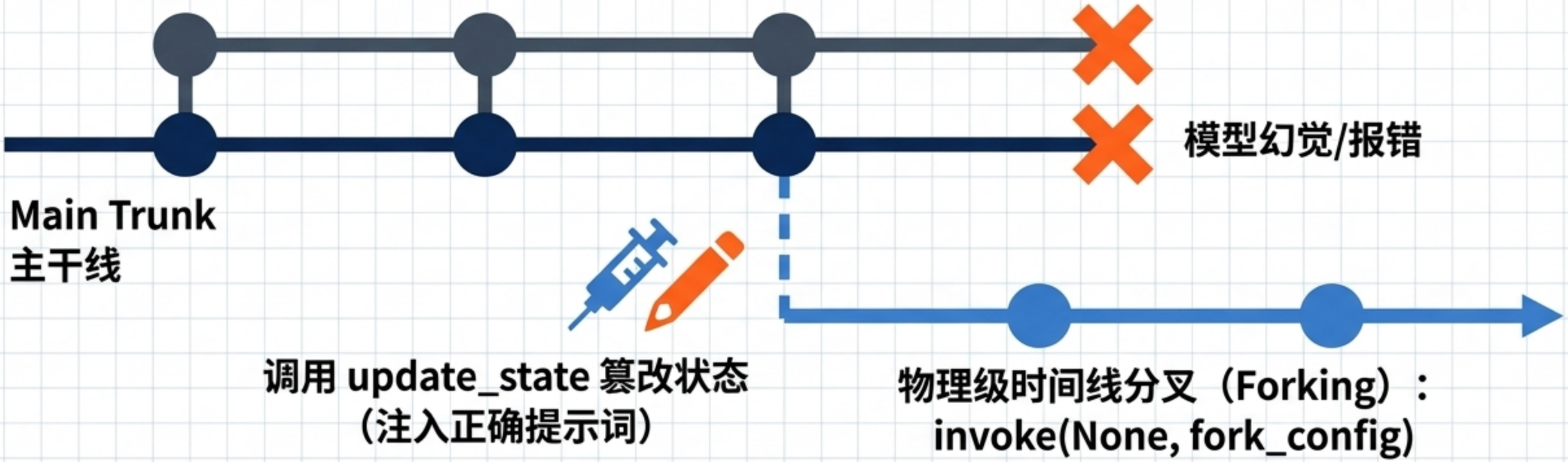
深度序列化为不可变快照
（Snapshot）

弹性物理存储生态

开发期：内存模式

生产期：PostgreSQL/Redis 高并发集群

时间线分叉（Forking）：物理级大模型无损排错



将非确定性的大模型黑盒排错，转化为可控的无损沙箱科学实验

体系化人机协同（Human-in-the-Loop）

人类专家决议：
Approve (放行) / Edit (修改) / Reject (驳回)

畅通

静态干预（硬卡点）：
interrupt_before/after
冻结进程入库

Security Gate

数据

挂起
(Suspended)

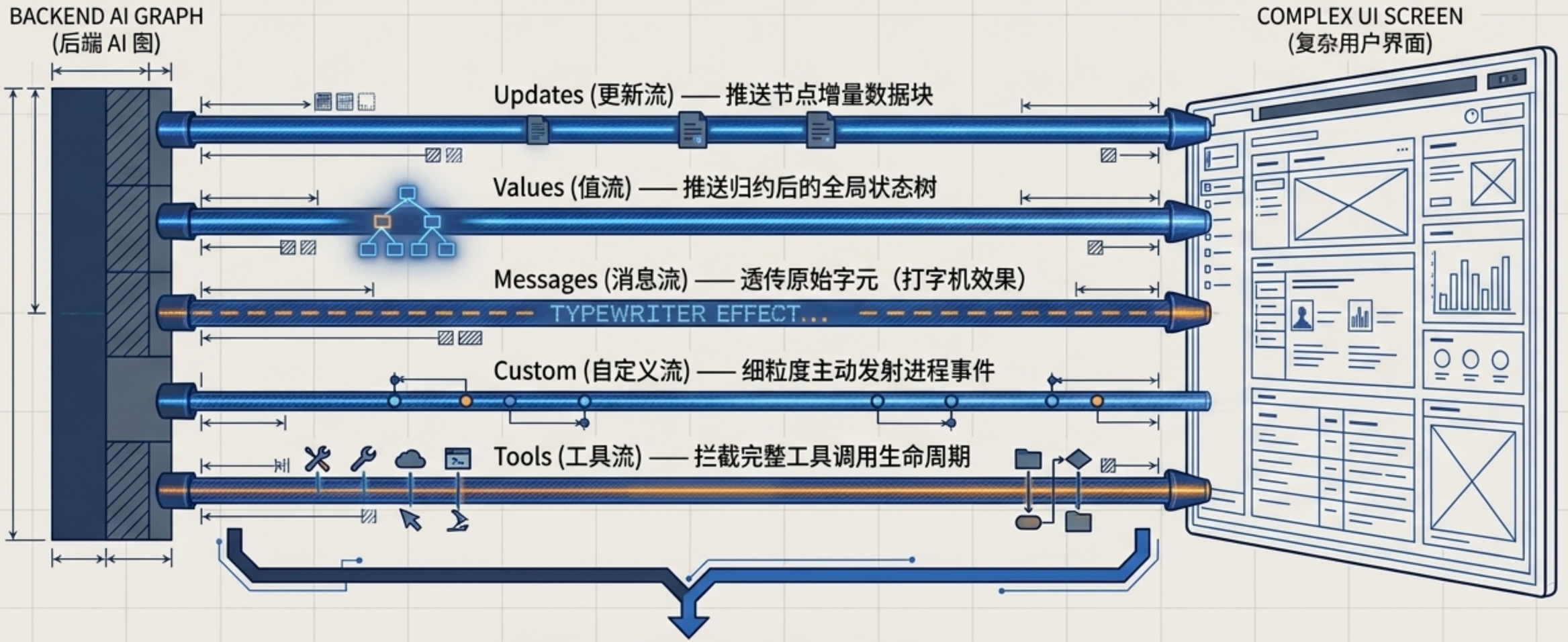
update_state
无损精准唤醒

高风险边界
（合同/邮件/改库）

动态干预（软挂起）：
interrupt()
基于模型不确定度随时挂起

ENGINEERING SPECIFICATION DOCUMENT	DRAWING NO. ARCH-2047	REVISION 1.0	DATE 2024-05-15

数据投影（Data Projection）：实时、低延迟的 AI 图到 UI 状态映射



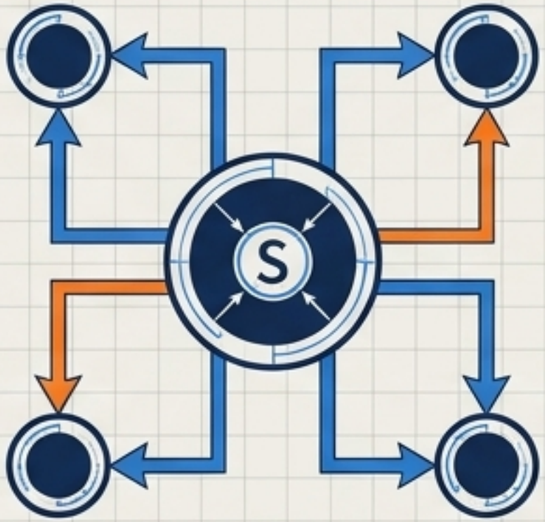
网络穿透：SSE 协议 + Metadata 解析

➡ 突破大模型首字节延迟（TTFT）局限

ENGINEERING SPECIFICATION DOCUMENT	DRAWING NO. ARCH-2047	REVISION 1.0	DATE 2024-05-15

多智能体（Multi-Agent）拓扑范式与上下文工程

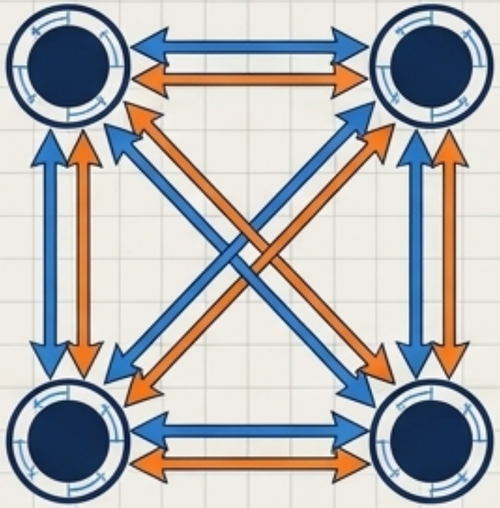
监督者模式（Supervisor）



监督者模式（Supervisor）

- 中心统筹，分发检验拦截
- 边界绝对清晰

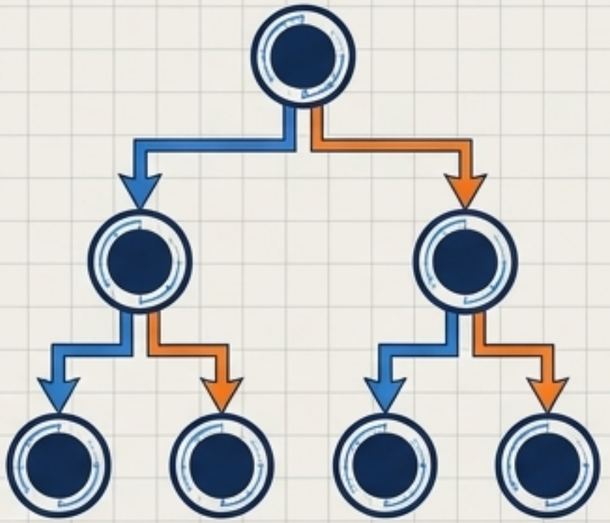
移交模式（Handoff）



移交模式（Handoff）

- 去中心化自主交棒
- 需强类型约束防范死锁内存尖峰

分层监督（Hierarchical）



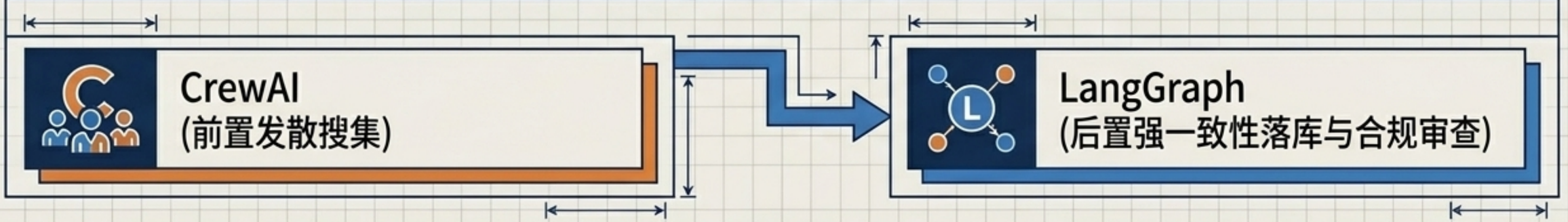
分层监督（Hierarchical）

- 总监 ➔ 主管 ➔ 员工
- 引入 MCP 协议跨物理边界异构集群

多智能体框架评估与混合架构

评估维度	LangGraph (企业级底盘)	CrewAI (敏捷原型)	AutoGen (对话辩论)
心智模型	图节点与状态边	拟人化角色与任务委派	多回合对话辩论循环
生产可靠性	【5/5 分】绝对确定性，原生快照	【3/5 分】深层委托易迷失	【3/5 分】易陷死循环致成本失控
可观测追踪	【5/5 分】全链路毫秒级执行树	【2/5 分】内部推演黑盒	【3/5 分】日志冗余解析难

混合架构解法



突破部署瓶颈：从本地实验室走向云原生企业级闭环生产